# 使用SAML配置Umbrella的ADFS版本3.0

## 目錄



## 簡介

本檔案介紹如何在Cisco Umbrella和Active Directory聯合身份驗證服務(ADFS)版本3.0之間配置SAML。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 概觀

本文介紹如何在Cisco Umbrella和Active Directory聯合身份驗證服務(ADFS)版本3.0之間配置SAML。使用ADFS配置SAML與Umbrella的其他SAML整合不同，因為它不是嚮導中的一兩次按一下過程，但需要對ADFS進行更改才能正常工作。

本文介紹為使SAML和ADFS協同工作而必須進行的詳細修改。主要步驟是先在ADFS環境和Cisco Umbrella之間禁用加密，然後將一些頒發轉換自定義宣告規則新增到Umbrella中繼方設定。

僅對現有的有效ADFS設定執行這些步驟。Cisco Umbrella支援無法提供幫助或支援，以幫助在特定環境中配置ADFS。

目前這些說明僅支援ADFS 3.0版(Windows Server 2012 R2)。可以將ADFS的更早版本（2.0或2.1）或更高版本(4.0)與Umbrella SAML整合配合使用，但該功能尚未經過測試或驗證。如果您有不同版本的ADFS，並且有意與我們的支援和產品團隊合作進行整合，請聯絡Cisco Umbrella支援。

您可以在Umbrella文檔中查詢初始SAML設定的先決條件：身份整合：前提條件。完成這些步驟後，您可以繼續使用本文中針對ADFS的說明來完成配置。

Umbrella文檔中的步驟提及您需要將SAML(ADFS)後設資料上傳到Umbrella。您可以通過導航到此URL然後上載XML檔案來訪問後設資料。

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

## 禁用加密

1.開啟AD FS管理。展開信任關係，然後選擇信賴方信任。

2.按一下右鍵Umbrella信賴方（或您為其命名的任意方），然後選擇Properties。

3.選擇Encryption頁籤。

4.選擇刪除以刪除證書以進行加密。

5.選擇OK關閉螢幕。

## 新增新的頒發轉換宣告規則

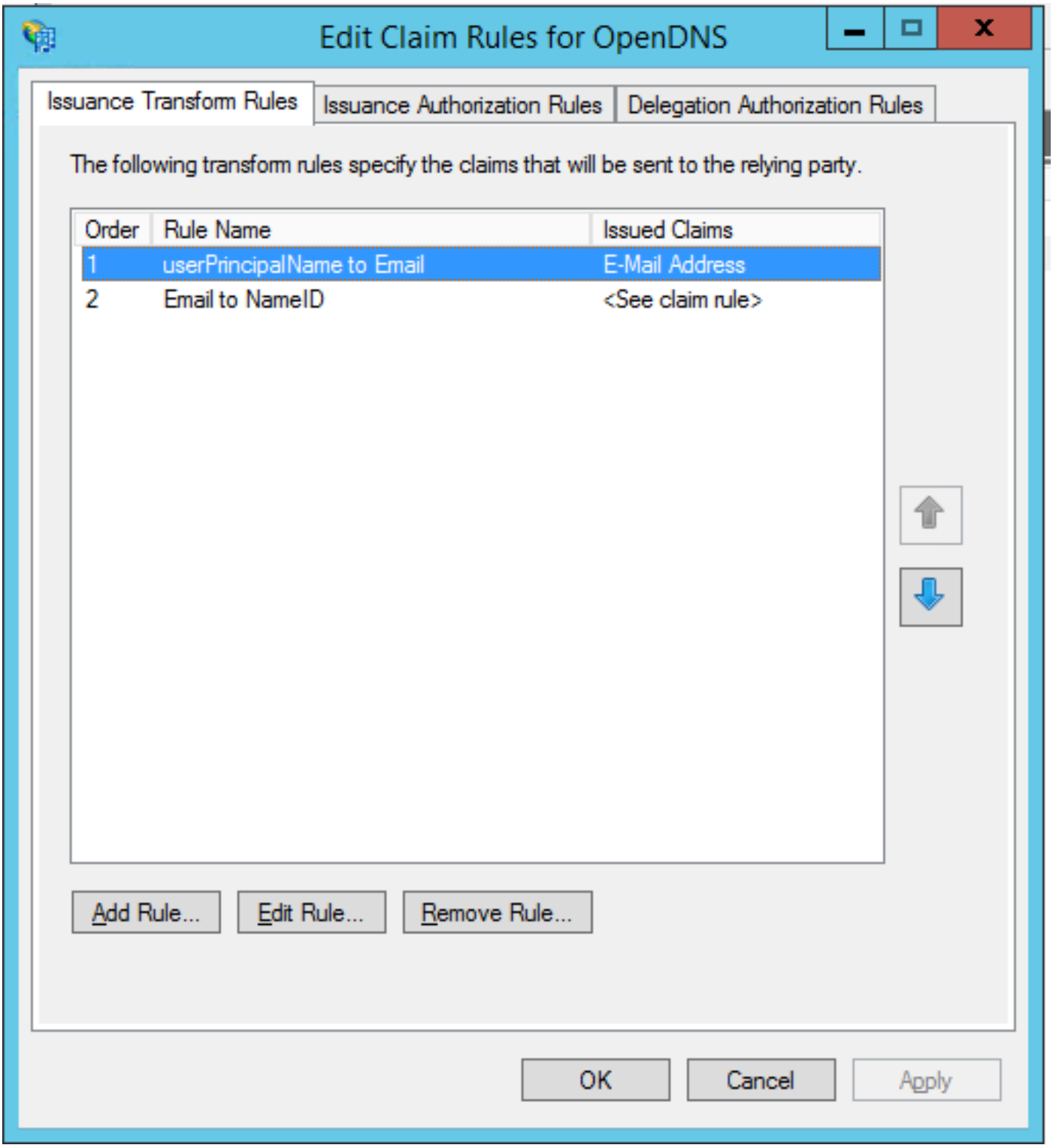
1.開啟AD FS管理。展開信任關係，然後選擇中繼方信任。

2.按一下右鍵Umbrella中繼方（或您指定的任何方），然後選擇「編輯宣告規則」。

3.在Issuance Transform Rules下，選擇Add Rule。

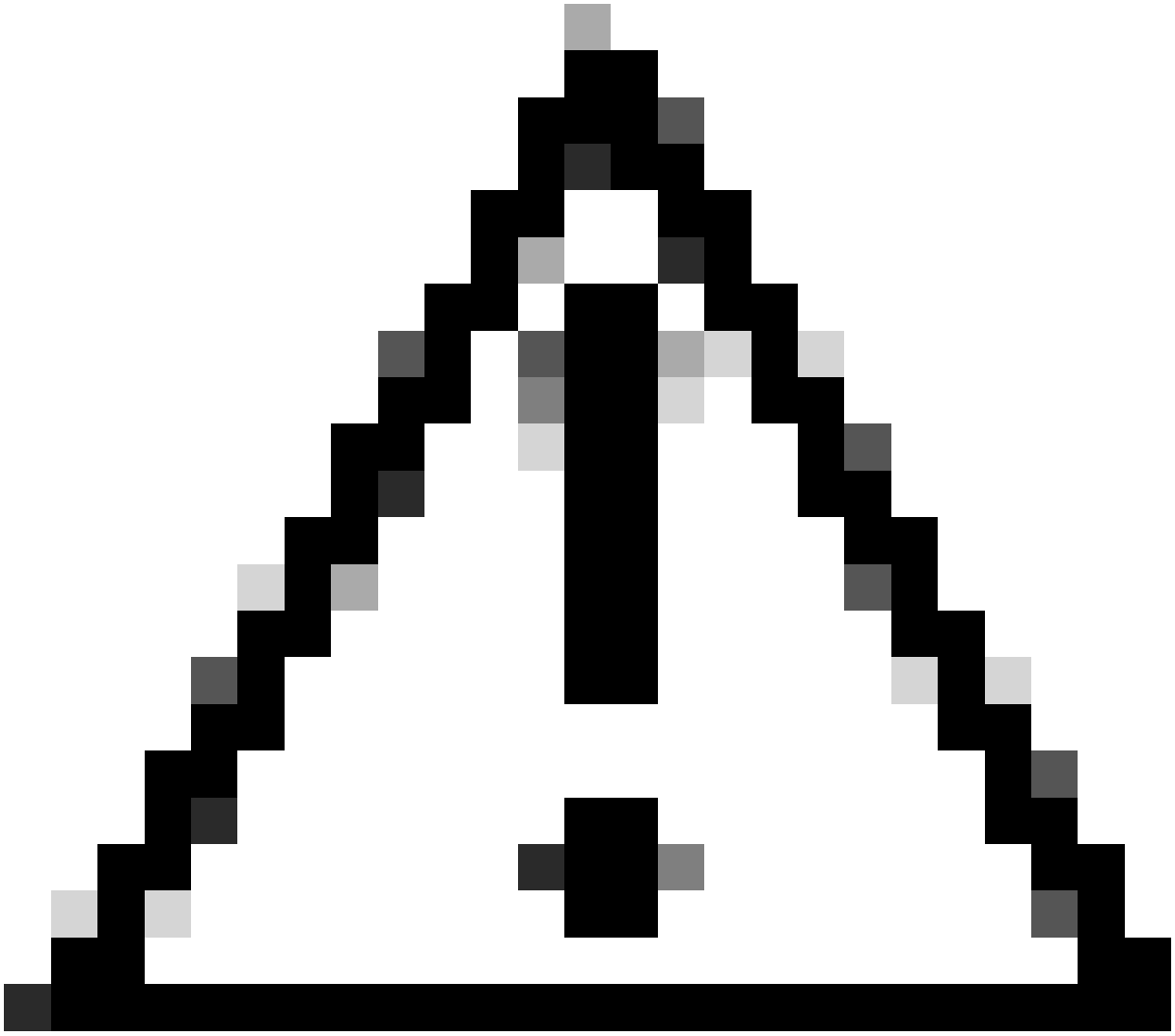
4.選擇「使用自定義規則傳送索賠」。

檢視此螢幕截圖，檢視您可以新增的規則清單。




新增這些規則後，整合即可開始工作。

## 轉換規則



注意：這些規則已經過測試，並在Umbrella的ADFS實驗室環境中以及一些客戶生產環境中運行。請根據您的環境進行修改。

---

userPrincipalName到電子郵件地址

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

傳送到名稱ID的電子郵件

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

# 附錄:使用「mail」屬性登入

預設情況下，ADFS通過使用者的UPN（使用者主體名稱）對使用者進行身份驗證。 如果您的使用者的電子郵件地址（Umbrella帳戶名稱）與其UPN不匹配，則需要執行其他步驟。請參閱此知識庫文章：如何在Cisco Umbrella Dashboard中配置AD FS以允許使用電子郵件地址登入？

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。